IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.	:	10/055,407	Confirmation No.: 7264
Applicants	:	David A. Fertell et al.	
Filed	:	January 23, 2002	
Title	:	**METHOD FOR MANAGING COMPUTER NETWORK ACCESS**	
Art Unit	:	2143	
Examiner	:	J. Bret Dennison	
Customer No.	:	28289	

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Dear Sir:

(I) REAL PARTY OF INTEREST

The real party of interest in this Appeal is Pearl Software, Inc., 64 East Uwchlan Avenue, Suite 230, Exton, Pennsylvania 19341.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to Commissioner for Patent, P.O. Box 1450, Alexandria, VA 22313-1450 on January 11, 2008.

Deborah L. Hartmann
(Name of Person Mailing Paper)

Deborah L. Hartmann 01/11/2008
Signature Date

01/15/2008 SDENBOB3 00000004 10055407
01 FC:2402 255.00 OP

Adjustment date: 01/15/2008 SDENBOB3
09/11/2006 MGEBREM1 00000112 10055407
01 FC:2402 -255.00 OP

LS6183.DOC

(II) RELATED APPEALS AND INTERFERENCES

None.

(III) STATUS OF THE CLAIMS

Claims 1-23 are pending. Claims 1-23 are appealed.

(IV) STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final rejection.

(V) SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 generally recites a method for controlling computer network access. The method includes (a) initiating at a client computer 1 a first communication session 100 at a first network address (paragraph 0052, lines 3-7, and Fig. 1); (b) receiving at the client computer 1 via the first communication 100 a second network address (paragraph 0052, lines 8-11); (c) initiating at the client computer 1 a second communication session 102 at the second network address (paragraph 0052, lines 12-15); (d) receiving at the client computer 1 via the second communication session 102 an access configuration (paragraph 0045 and paragraph 0053, lines 1-5) including a control setting for at least one communication protocol capable of being utilized (paragraph 0054 through paragraph 0057, and Fig. 2) during a third communication session 104; (e) instantiating on the client computer 1 a process which initiates a third communication session 104 at a third network address (paragraph 0055, lines 1-3); and (f) in connection with the third communication session 104, controlling the conveyance of data either to or from the process instantiated on the client computer 1 based on the control setting for the one communication protocol (paragraph 0055, lines 3-21).

Claim 7 depends from claim 1 and includes at least one of the following steps: after (b), terminating the first communication session 100 (paragraph 0053, lines 1 and 2); and/or after step (d), terminating the second communication session 102 (paragraph 0075, lines 1-5).

Claim 8 depends from claim 1 and includes the further steps of: transmitting from the client computer 1 via the second communication session 102 a request to receive

another access configuration including a control setting for the one communication protocol (paragraphs 0011 and 0070); receiving at the client computer 1 via the second communication session 102 the other access configuration (paragraphs 0011 and 0070); and performing step (f) based on the control setting included in the other access configuration (paragraph 0011, lines 4-6).

Claim 10 depends from claim 9 and includes the further step of transferring at least part of the conveyed data to the second network address via the second communication session 102 (paragraph 0057, lines 1-4).

Independent claim 13 generally recites a method for controlling computer network access that includes the steps of: (a) storing at a client computer 1 a first network address 100 (paragraph 0052, lines 5-8, Fig. 1); (b) initiating a first communication session between the client computer 1 and a first server computer 2 at the first network address 100 (paragraph 0052, lines 5-7, Fig. 1); (c) receiving at the client computer 1 from the first server computer 2 via the first communication session a second network address 102 or 102N (paragraph 0052, lines 8-11, Fig. 1); (d) initiating a second communication session between the client computer 1 and a second server computer 2 or 5 at the second network address 102 or 102N (paragraph 0052, lines 12-17, Fig. 1); (e) receiving at the client computer 1 from the second server computer 102 or 102N an access configuration (paragraph 0053, lines 1-5, Fig. 1) including a control setting for at least one communication protocol capable of being utilized during a third communication session 104 (paragraphs 0054-0057); (f) instantiating on the client computer 1 concurrent with the second communication session a process which initiates a third communication session 104 between the client computer 1 and a remote computer 3 at a third network address (paragraph 0055, lines 1-3, Fig. 1); and (g) in connection with the third communication session 104, controlling data conveyed at least one of (i) to and (ii) from the instantiated process on the client computer 1 based on the control setting for the one communication protocol (paragraph 0055, lines 3-21, Figs. 1-3a).

Claim 15 depends from claim 13 and includes at least one of the following steps: after step (c) the step of terminating the first communication session 100 (paragraph 0053, lines 1 and 2); and/or after step (e), terminating the second communication session 102 (paragraph 0075, lines 1-5).

Claim 18 depends from claim 13 and includes the further steps of: initiating at the client computer 1 via the second communication session 102 a request to the second server computer 2 or 5 to transmit another access configuration (paragraphs 0011 and 0070); receiving at the client computer 1 from the second server computer 2 or 5 the other access configuration (paragraphs 0011 and 0070); and performing step (g) based on a control setting included in the other access configuration for the one communication protocol (paragraph 0011, lines 4-6).

Independent claim 22 recites a method of controlling computer network access comprising: (a) initiating a communication session 102 between a first computer 1 and a second computer 2 or 5 (paragraph 0052, lines 8-17); (b) receiving at the first computer 1 from the second computer 2 or 5 via the communication session 102 an access configuration including a control setting for at least one communication protocol (paragraph 0053, lines 1-5, Fig. 1); (c) monitoring data conveyed to or from a process running on the first computer 1 based on the control setting (paragraph 0055, lines 3 and 4); and (d) controlling the data conveyed to or from the process based on the control setting (paragraph 0055, lines 5-21).

Claim 23 depends from claim 22 and includes the further limitation that the process instantiates another computer communication session 104 (paragraph 0055, lines 1-3); and the conveyance of data is controlled in connection with the other communication session 104 (paragraph 0055, lines 3-21).

(VI) GROUND(S) OF REJECTION TO BE REVIEWED ON APPEAL

Are claims 22 and 23 anticipated under 35 U.S.C. § 102(e) from the teachings of U.S. Patent document 7,113,994 to Swift et al. ?

Are claims 1-9 and 13-21 obvious under 35 U.S.C. § 103(a) from the teachings of the Swift et al. document in view of U.S. Patent document 2006/0077977 to Caronni et al. ?

(VII) ARGUMENT

In accordance with 37 C.F.R. § 41.37(c)(VII), it is respectfully requested that the patentability of each claim argued separately be considered separately.

Claims 10-12:

Applicants acknowledge with appreciation the indication that claims 10-12 would be allowable if rewritten in independent form including all the limitations of the base claim and any intervening claims. For the reasons discussed hereinafter, it is believed that amendments to claims 10-12 are not necessary in order to place them in condition for allowance.

Claims 1 and 13:

Claim 1 generally recites a method for controlling computer network access. The method includes initiating at a client computer a first communication session at a first network address and receiving at the client computer via the first communication session a second network address. A second communication session is initiated at the client computer at the second network address. The client computer receives via the second communication session an access configuration including a control setting for at least one communication protocol capable of being utilized during a third communication session. A process is instantiated on the client computer which initiates a third communication session at a third network address. In connection with the third communication session, the conveyance of data to or from the process instantiated on the client computer is controlled based on the control setting for the one communication protocol.

In rejecting independent claims 1 and 13, the Examiner alleges, among other things, that the Swift et al. document discloses steps (c), (d), (e) and (f) of claim 1. The Examiner also admits that the Swift et al. document does not disclose steps (a) and (b) of claim 1. However, the Examiner alleges that the Caronni et al. document discloses ". . . a system and method where a web client 1102 obtains an address to a web server1104 [sic] from computer system 1106 (Caronni, Fig. 11, [0079])."

In applying the teachings of the Swift et al. document to the rejection of claim 1, the Examiner equates the proxy client 74 in Fig. 2 of the Swift et al. document with the client computer of the steps of claim 1. A fair reading of the Swift et al. document, however, discloses that proxy client 74 enables a client (not a user) to authenticate himself for accessing a service 76 on behalf of a user (see Swift et al., column 5, lines 4-11). What is clear from the Swift et al. document, however, is that user 70, whose computer appears next to user 70 in Fig.

2 of the Swift et al. document, is not the same party as proxy client 74 in Fig. 2 of the Swift et al. document. To this end, the Swift et al. document itself makes a distinction between user 70 and proxy client 74. Accordingly, it is believed that equating proxy client 74 in the Swift et al. document with the client computer in claim 1 is improper.

Notwithstanding, in the Swift et al. document, proxy client 74 accesses target service 76 by first requesting credentials from a trusted security server 80 that either (1) returns the credentials to proxy client 74 for proxy client 74 to pass on to target service 76 for authentication/access purposes or (2) passes the credentials directly to target service 76 in anticipation of the login request from proxy client 74. In contrast, in the method of claim 1, the conveyance of data to or from a process instantiated on a client computer is controlled based on a control setting included in an access configuration stored at the client computer. Stated differently, in the Swift et al. document, access to target service 76 is controlled at target service 76 itself. In contrast, in claim 1 access is controlled at the client computer which the Examiner equates with proxy client 74 in the Swift et al. document. In other words, the Swift et al. document discloses, teaches and suggests controlling access and, hence, the conveyance of data, at a completely different location than the control of conveyance of data in claim 1 which is controlled by the control setting received at the client computer. Accordingly, the Swift et al. document cannot disclose, teach or suggest the limitations of steps (c)-(f) of claim 1 as alleged by the Examiner.

The Caronni et al. document does not cure the foregoing deficiencies in the teachings of the Swift et al. document.

Turning now to the application of the Caronni et al. document to the rejection of claim 1, ". . . a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. Although common sense directs one to look with care at a patent application that claims as an innovation the combination of two known devices according to their established functions, it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. This is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is

already known." KSR Int'l Co., v. Teleflex, Inc., No. 04-1350, slip op. at 14-15 (U.S. Apr. 30, 2007).

Moreover, in making the assessment of differences, section 103 specifically requires consideration of the claimed invention as a whole. Ruiz v. A.B. Chance Co., 357 F.3d 1270, 69 USPQ2d 1686 (Fed. Cir. 2004).

There is no disclosure, teaching or suggestion in the Swift et al. and Caronni et al. documents to merge their respective teachings in the manner suggested by the Examiner to arrive at the invention claimed as a whole in claim 1. To this end, in applying the teachings of the Caronni et al. document to the rejection of claim 1, the Examiner's reasoning necessarily relies upon the limitations of claim 1, namely, steps (a) and (b) of claim 1, to establish the need for the limitations thereof. Based on this, the Examiner argues that the need for these limitations would have motivated one to search the prior art for well-known techniques for discovering devices or obtaining addresses of devices on the network. The Examiner then concludes that the Caronni et al. document supplies this teaching. However, other than the disclosure in the present application of the limitations of claim 1 as a whole, there is no motivation disclosed in the Swift et al. and Caronni et al. documents to combine their respective teachings in the manner suggested by the Examiner in the rejection of claim 1.

To this end, the Swift et al. document discloses no need to initiate at a client computer a first communication session at a first network address and receive at the client computer via the first communication the second network address. Assuming *arguendo*, the Caronni et al. document discloses these features, there is no apparent reason disclosed in either the Swift et al. and/or Caronni et al. documents that establishing a first communication session in order to receive a second network address for the purpose of initiating a second communication session for receiving an access configuration to control yet a third communication session at the third network address is disclosed, taught or suggested in the combination of the Swift et al. and Caronni et al. documents.

Furthermore, the Examiner has not explained why one would choose the teachings of the Caronni et al. document over other techniques that may exist in the prior art. For example, the second address could be made known in another manner, e.g., orally, by telephone, etc. Moreover, the Examiner has not explained why one would use the first communication session for the sole purpose of obtaining a second network address for a second

communication session. To this end, it is just as speculative that the client could have learned of the second network address during a first communication session and, thereafter, utilized the first communication session, instead of a second communication session, to receive the access configuration including a control setting.

Thus, as can be seen, there is no motivation to combine the teachings of the Swift et al. and Caronni et al. documents in the manner suggested by the Examiner in the Office Action to arrive at the invention claimed as a whole in claim 1.

Furthermore, it is not clear how the teachings of the Caronni et al. document can be combined with the teachings of the Swift et al. document. Specifically, as discussed above, control of access to the target service 76 in the Swift et al. document is controlled by target service 76, not proxy client 74. However, as best understood, the information that target service 76 bases its decision to either enable or block access is provided by user 70, not proxy client 74. Accordingly, the teachings of the Caronni et al. document are not logically combinable with the teachings of the Swift et al. document. "[K]nowledge in the prior art of every element of a patent claim . . . is not of itself sufficient to render [a] claim obvious. Graham v. John Deere Co., 383 U.S. 1, 17-18 (1966); Teleflex, Inc. v. Ficosa N. Am. Corp., 299 F.3d 1313, 1333-34 (Fed. Cir. 2002). The issue is whether substantial evidence supports the judgment (under the clear and convincing evidence standard) that a person having ordinary skill in the art would not have been motivated to replace the [prior art] combination ... with [the claimed combination.]" Abbott Laboratories v. Syntron Bioresearch, Inc., 334 F.3d 1343, 67 USPQ2d 1337 (Fed. Cir. 2003).

As can be seen, there is no apparent reason to combine the teachings of the Swift et al. document and the Caronni et al. document in the manner suggested by the Examiner to arrive at the invention of claim 1. To this end, "Prior knowledge in the field of the invention must be supported by tangible teachings of reference materials, and the suggestion to combine references must not be derived by hindsight from knowledge of the invention itself." Cardiac Pacemakers v. St. Jude Medical, Inc., 381 F.3d 1371 (Fed. Cir. 2004).

In addition, there is no disclosure, teaching or suggestion in the Swift et al. and Caronni et al. documents, either individually or in combination, to provide a first communication session between a client computer and a first server computer and to initiate a second communication session between the client computer and a second server computer as

claimed in claim 13. This is admitted by the Examiner in the rejection of claim 14, wherein the Examiner states that "the first and second server computers are the same server computer" (Swift et al., Fig. 2, 80)."

For the foregoing reasons, the Swift et al. and Caronni et al. documents, either individually or in combination, cannot anticipate or render obvious claim 1 of the present application, or claims 2-12 dependent therefrom. Similarly, for the reasons discussed above in connection with claim 1, the Swift et al. and Caronni et al. documents, either individually or in combination, cannot anticipate or render obvious claim 13 of the present application, or claims 14-21 dependent therefrom.

Claims 8 and 18:

In the rejection of claims 8 and 18, the Examiner argues that ". . . it would have been obvious to one of ordinary skill in the art at the time the invention was made to repeat the steps in Swift et al. and Caronni et al. in order to obtain authorization for other target services." As noted above in connection with claim 1, the Swift et al. document discloses that target service 76 performs the access control function. There is simply no disclosure, teaching or suggestion in the Swift et al. and Caronni et al. documents, either individually or in combination, to provide another access configuration. Accordingly, notwithstanding that target service 76 performs access control in the Swift et al. document, it is respectfully submitted that the Examiner's conclusion in the rejection of claims 8 and 18 is based on hindsight.

Claim 22:

Independent claim 22 recites a method of controlling computer network access. The method includes: (a) initiating a communication session between a first computer and a second computer; (b) receiving at the first computer from the second computer via the communication session an access configuration including a control setting for at least one communication protocol; (c) monitoring data conveyed to or from a process running on the first computer based on the control setting; and (d) controlling the data conveyed to or from the process based on the control setting.

As discussed above in connection with the rejection of claim 1, the controlling of data between target service 76 and proxy client 74 is controlled by target service 76, not proxy client 74. There is no disclosure teaching or suggestion in the Swift et al. document how target service 76 receives its access configuration including a control setting that is utilized to control the conveyance of data. Accordingly, the Swift et al. document cannot anticipate claim 22 of the present application.

CONCLUSION

As can be seen, the Swift et al. and Caronni et al. documents, either individually or in combination, do not disclose, teach or suggest a method having all the limitations of claims 1-23. Accordingly, these documents cannot render obvious claims 1-23 of the present application.

It is respectfully urged that the final rejection on the merits be reversed and a Notice of Allowance issued.

A check in the amount of $5.00 is enclosed to cover the difference between the current 37 C.F.R. § 41.20(b)(2) fee for filing an Appeal Brief and the fee in effect at the time of filing an original Appeal Brief filed in connection with the application on September 7, 2006.

The Commissioner for Patents is hereby authorized to charge any additional fees which may be required to Deposit Account No. 23-0650. Please refund any overpayments to Deposit Account No. 23-0650.

Respectfully submitted,

THE WEBB LAW FIRM

By _____

William H. Logsdon
Registration No. 22,132
Attorney for Applicants
700 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219
Telephone: 412-471-8815
Facsimile: 412-471-4094
E-Mail: webblaw@webblaw.com

(VIII) CLAIM APPENDIX

1. A method for controlling computer network access, the method comprising the steps of:

(a) initiating at a client computer a first communication session at a first network address;

(b) receiving at the client computer via the first communication session a second network address;

(c) initiating at the client computer a second communication session at the second network address;

(d) receiving at the client computer via the second communication session an access configuration including a control setting for at least one communication protocol capable of being utilized during a third communication session;

(e) instantiating on the client computer a process which initiates a third communication session at a third network address; and

(f) in connection with the third communication session, controlling the conveyance of data at least one of (i) to and (ii) from the process instantiated on the client computer based on the control setting for the one communication protocol.

2. The method as set forth in claim 1, wherein:

the access configuration includes a list related to the control setting for the one communication protocol; and

the conveyance of data via the third communication session is controlled based on the list.

3. The method as set forth in claim 1, wherein the one communication protocol includes one of:

World Wide Web (Web);

file transfer protocol (FTP);

E-mail;

News;

Chat;

Instant Messaging;

Telnet; and

Peer-to-Peer.

4. The method as set forth in claim 1, wherein the control setting is one of:

unrestricted computer network access (Allow All);

no computer network access (Block All);

limited computer network access to network addresses included in an allow list (Allow Listed); and

unrestricted computer network access except to network addresses included in a block list (Block Listed).

5. The method as set forth in claim 1, wherein:

the access configuration further includes at least one of the following global control settings:

access prohibited to conveyed data including a predetermined word or phrase;

access prohibited to data of at least one predetermined data type;

access prohibited to data conveyed during at least one of a predetermined time and day-of-week; and

access prohibited based on a rating for a category included with the conveyed data;

and

step (f) further includes the step of controlling the conveyance of data at least one of (i) to and (ii) from the process instantiated on the client computer based on the at least one global control setting.

6. The method as set forth in claim 5, wherein the at least one predetermined data type includes an Internet cookie.

7. The method as set forth in claim 1, further including at least one of:

after step (b), the step of terminating the first communication session; and

after step (d), the step of terminating the second communication session.

8. The method as set forth in claim 1, further including the steps of:

transmitting from the client computer via the second communication session a request to receive another access configuration including a control setting for the one communication protocol;

receiving at the client computer via the second communication session the other access configuration; and

performing step (f) based on the control setting included in the other access configuration.

9. The method as set forth in claim 1, wherein step (f) further includes the steps of:

determining from the conveyed data the communication protocol thereof; and

determining from the thus determined communication protocol the control setting therefor.

10. The method as set forth in claim 9, further including the step of transferring at least part of the conveyed data to the second network address via the second communication session.

11. The method as set forth in claim 10, wherein the transferred data includes at least one of the following:

a network address; and

a subject of the third communication session.

12. The method as set forth in claim 10, further including the step of transferring with the data a login name received by the client computer during a login procedure by a user thereof.

13. A method for controlling computer network access comprising the steps of:

(a) storing at a client computer a first network address;

(b) initiating a first communication session between the client computer and a first server computer at the first network address;

(c) receiving at the client computer from the first server computer via the first communication session a second network address;

(d) initiating a second communication session between the client computer and a second server computer at the second network address;

(e) receiving at the client computer from the second server computer an access configuration including a control setting for at least one communication protocol capable of being utilized during a third communication session;

(f) instantiating on the client computer concurrent with the second communication session a process which initiates a third communication session between the client computer and a remote computer at a third network address; and

(g) in connection with the third communication session, controlling data conveyed at least one of (i) to and (ii) from the instantiated process on the client computer based on the control setting for the one communication protocol.

14. The method as set forth in claim 13, wherein the first and second server computers are the same server computer.

15. The method as set forth in claim 13, further including at least one of:

after step (c), the step of terminating the first communication session; and

after step (e), terminating the second communication session.

16. The method as set forth in claim 13, wherein:

the access configuration further includes at least one of the following global control settings:

access prohibited to conveyed data including at least one of a predetermined word and a predetermined phrase;

access prohibited to data including at least one predetermined data type;

access prohibited to data conveyed during at least one of a predetermined time and day-of-week; and

access prohibited based on a rating for a category included with the computer data;

and

step (g) further includes the step of controlling the conveyance of data at least one of (i) to and (ii) from the process instantiated on the client computer based on the at least one global control setting.

17. The method as set forth in claim 16, wherein:

prior to receipt of the access configuration at the client computer, the control setting for the one communication protocol is selected from a plurality of different control settings therefor; and

each global control setting is selected nonexclusively of any other global control settings.

18. The method as set forth in claim 13, further including the steps of:

initiating at the client computer via the second communication session a request to the second server computer to transmit another access configuration;

receiving at the client computer from the second server computer the other access configuration; and

performing step (g) based on a control setting included in the other access configuration for the one communication protocol.

19. The method as set forth in claim 13, wherein:

the access configuration includes for the control setting for the one communication protocol a list; and

the conveyance of data in step (g) is controlled based upon an entry included in the list.

20. The method as set forth in claim 19, wherein the entry comprises a network address.

21. The method as set forth in claim 13, further including the step of determining the communication protocol from the conveyed data.

22. A method of controlling computer network access comprising:

(a) initiating a communication session between a first computer and a second computer;

(b) receiving at the first computer from the second computer via the communication session an access configuration including a control setting for at least one communication protocol;

(c) monitoring data conveyed to or from a process running on the first computer based on the control setting; and

(d) controlling the data conveyed to or from the process based on the control setting.

23. The method of claim 22, wherein:

the process instantiates another communication session; and

the conveyance of data is controlled in connection with the other communication session.

(IX) EVIDENCE APPENDIX

NONE

(X) RELATED PROCEEDINGS APPENDIX

NONE